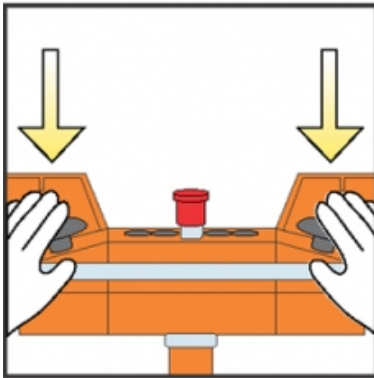


Safety Chain Solution – Multifunction - Two-hand control

PL e, SIL 3

Complex machine applications using a centralized safety device



Function:

- Safety-related function to help control the location of the operator's hands outside the hazardous area during a hazardous movement of the machine.
- To initiate a movement, both actuators (two-hand control pushbuttons S3 and S4) must be activated synchronously (within an interval less than 0,5 sec.) to energize the contactors (K1 and K2). When at least one of the two pushbuttons is released, the energization is cancelled and remains blocked until both pushbuttons are released and pressed again synchronously.
- The logic device (Safety Controller) monitors operation of the actuators (pushbuttons). Faults in the actuating mechanism as well as the cable wiring are detected in S3/S4 by the use of two contacts employing a normally open (NO) and normally closed (NC) combination.
- Faults in K1/K2 (with mirror contacts) are detected in the safety controller and lead to de-energization of the contactors (K1 and K2).



Typical applications:

- Hydraulic, eccentric press or similar complex machines with 4 or more safety functions included, where a centralized safety controller would be required.

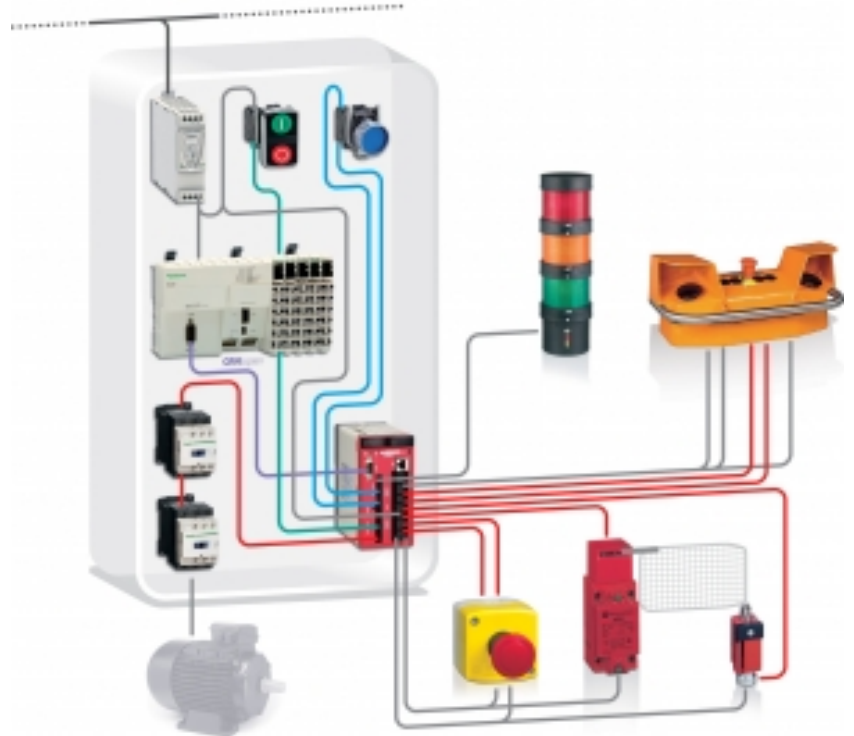
Safety Chain Solution – Multifunction - Two-hand control

Design:

- The safety function employs well-tried safety principles and is robust in the event of a component failure by means of two redundant contacts of each actuator (pushbutton) and two redundant contactors (K1 and K2).
- The contacts of the actuators S3/S4 of the two-hand control must satisfy EN/IEC 60947-5-1. Due to the low currents, pushbuttons with gold-plated contacts are recommended.
- The actuators of the control stations must be designed and installed such that they cannot be activated involuntarily or easily rendered inoperative, in accordance with EN 574/ ISO 13851.
- The design of the control station must incorporate features to significantly reduce occupational illnesses associated with repetitive movements of the hands.
- The control stations must be located at a point from which the potential danger is visible. The safety distance between the control units and the hazardous zone must be sufficient to ensure that the hazard cannot be reached by the operator before the dangerous movement has been completed or stopped.
- The safety controller satisfies the requirements for performance level PL e in accordance with EN ISO 13849-1 and SIL 3 in accordance with EN/IEC 61508. This device includes the two-hand control safety function that corresponds to Type III C in accordance with EN 574/ISO 13851.
- The contactors (K1 and K2) are considered as well-tried components.
- Protection against overcurrent must be provided in accordance with EN/IEC 60947-4-1.
- The contactors (K1 and K2) have mirror contacts in accordance with EN/IEC 60947-4-1, which are integrated into the input of the safety controller for fault detection.
- Depending on the application, the requirements of type C standards (such as EN692 for mechanical presses) specific to the machinery involved must be met, and additional protective equipment may have to be considered.

Related products

- Switches, pushbuttons - [Harmony XB4](#)
- Emergency stop control station - [Harmony XALK](#)
- Two-Hand control station - [Preventa XY2SB](#)
- Switch mode Power supply - [Phaseo ABL8](#)
- Logic controller - [Modicon M258](#)
- Guard interlock switch - [Preventa XCS](#)
- Safety Controller - [Preventa XPS MC](#)
- Contactor - [TeSys D](#)
- Modular beacon and tower light - [Harmony XVB](#)



Safety Chain Solution – Multifunction - Two-hand

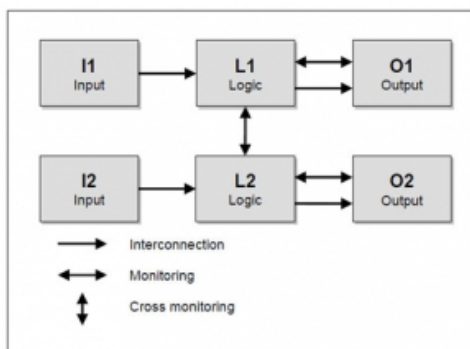
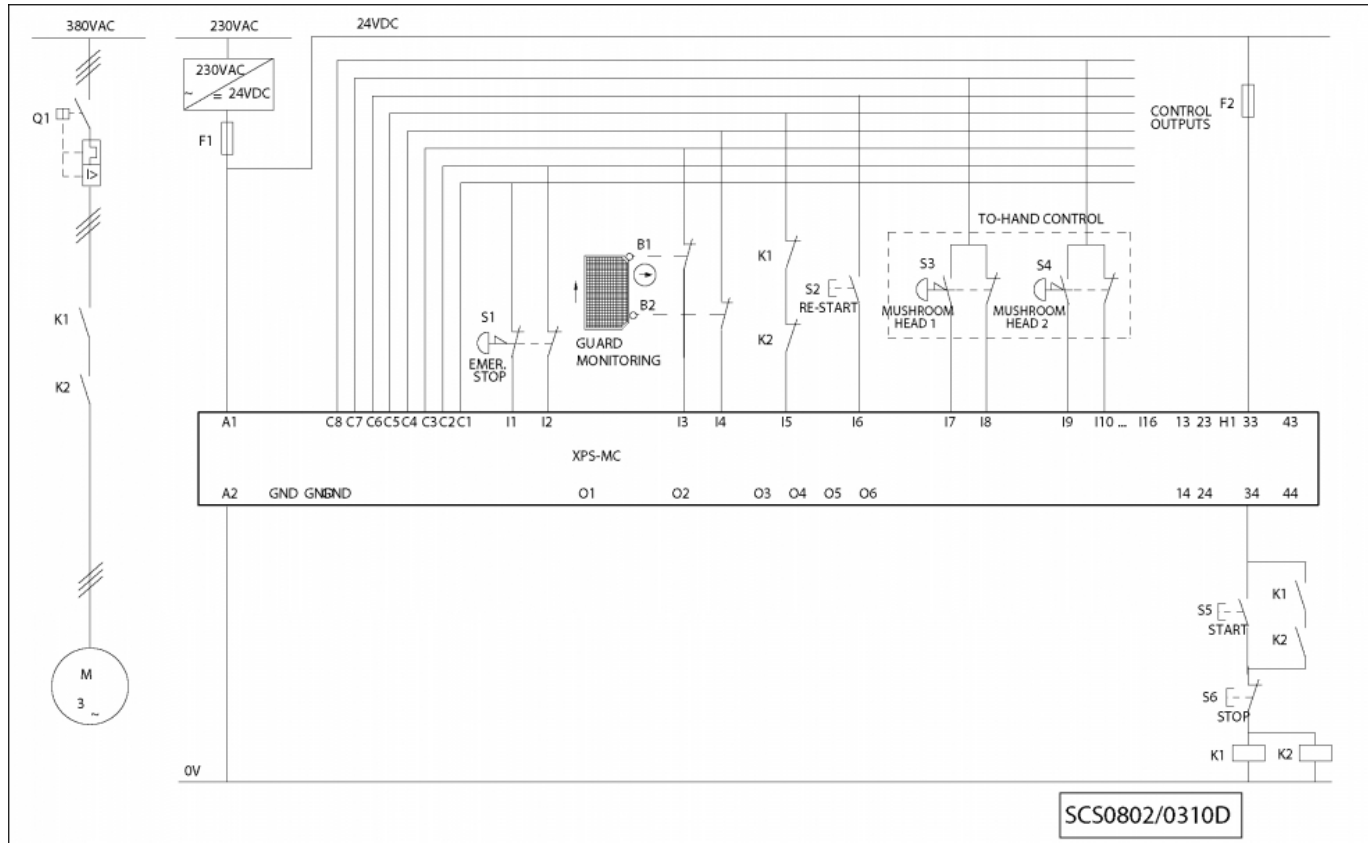


Figure 1

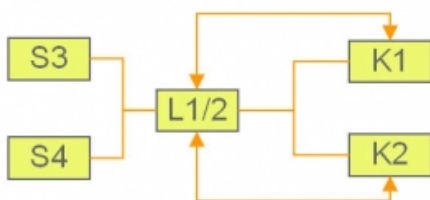


Figure 2

Chain structure:

- The circuit diagram SCS0802/0310D is a conceptual schematic diagram and is presented to illustrate the safety function with only the relevant safety components shown.
- For the designated architecture of the category 4 system, two redundant channels are implemented.
- The circuit arrangement can be divided into three function blocks, input (I), logic (L) and output (O) blocks, per channel.
- The unbroken lines for monitoring symbolize the higher DCavg assumed for this category (see figure 1).
- The functional channel is represented by the two-hand control actuator device (S3 and S4) that corresponds to the input block (see figure 2).
- The safety controller (XPSMC) corresponds to the logic block (L1/2), which maintains the internal redundancy of the safety circuits required for this category.
- The output is represented by two redundant contactors (K1 and K2) that are monitored by the logic block (safety modules) to detect failure.
- The complete wiring must be in accordance with EN/IEC 60204-1 and measures to avoid short circuits have to be provided (EN ISO 13849-2 Table D.4).

Safety Chain Solution – Multifunction - Two-hand control

Safety level calculation:

Cycle time (s)	10
Number of hours' operation per day (h)	12
Number of days' operation per year	220
Number of operations per year (n_{op})	950400

		Values	
		Channel 1	Channel 2
Input (Two-hand control) XY2S	B10 _d (operations)	25 000 000	25 000 000
	T10 _d (years)	26.3	26.3
	MTTF _d (years)	263.05	263.05
	MTTF _d resulting (years)	131.5	131.5
	PFH _d resulting (1/h)	1.85×10^{-8}	1.85×10^{-8}
	DC (%)	99	99
Logic (safety controller) XPSMC	PFH _d (1/h)	1.4×10^{-8}	1.4×10^{-8}
Output (actuator) LC1	B10 (operations)	10 000 000	10 000 000
	% dangerous failure	50	50
	B10 _d (operations)	20 000 000	20 000 000
	T10 _d (years)	21.04	21.04
	MTTF _d (years)	210.4	210.4
	MTTF _d resulting (years)	210.4	210.4
	PFH _d resulting (1/h)	1.13×10^{-8}	1.13×10^{-8}
	DC (%)	99	99
Safety function	MTTF _{dC}	32.6 (high)	
	DC _{avg}	99 (high)	
	PFH _d resulting (1/h)	4.37×10^{-8}	
	PL attained	e	
	SIL attained	3	

- A required performance level (PLr) must be specified for each intended safety function following a risk evaluation. The performance level (PL) attained by the control system must be validated by verifying if it is greater than or equal to the PLr.
- If the two-hand control station is assumed to be actuated every 10 seconds during 220 working days per year and 12 working hours, the number of operations (n_{op}) would be 950 400 per year.
- A B10d value of 25 000 000 cycles is stated for each pushbutton contact. In accordance with the assumed above n_{op} value, the MTTF_d would be 263.05 years for this element. As we need 2 contacts for each actuator the MTTF_d resulting for channel 1 would be 131.5 years. A similar result would be achieved for channel 2.
- A PFH_d value of 1.4×10^{-8} is stated for the safety controller (XPSMC). This value comes directly from the safety device data and it is certified by a notified body.
- For the redundant contactors K1 and K2, the B10 value corresponds under low load to an electrical lifetime of 10 000 000 switching cycles. If 50% of failures are assumed to be dangerous, the B10d values is 20 000 000 operations. With the assumed value for n_{op} , it results in a MTTF_d of 210.4 years for each component. These values are not limited in this case as this is a category 4 system and they are under the 2500 year limit used by the SISTEMA calculation tool.
- Measures against common cause failures must attain at least 65 points (i.e. separation (15), diversity (20), over voltage protection etc. (15) and environmental conditions (25+10)).
- Since this is the highest performance level, both the MTTF_d of each channel and the DC_{avg} must be high.
- The combination of channel 1 and channel 2 results in a DC_{avg} 99% (high) as we are monitoring the combination of actuator contacts in the two-hand control station and using mirror contact monitoring for the contactors.
- The safety-related control system corresponds to category 4 with high MTTF_d. The complete safety chain results in an average probability of dangerous failure (PFH_d) of 4.37×10^{-8} .
- This corresponds to PL e and SIL 3.

SCS0802/0310 - 03-03-2010

ATTENTION

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric Industries SAS nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein.

Schneider Electric Industries S.A.S

Head Office
35 rue Joseph Monier
CS 30323
92506 Rueil-Malmaison
www.schneider-electric.com

As standards, specifications and designs change from time to time, please ask for confirmation of the information given in this publication.

Design : Schneider Electric
Photos : Schneider Electric